This listing of claims will replace all prior versions, and listings of claims in the application:

**LISTING OF CLAIMS:**

1. (Currently Amended) A method for generating a shared key comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters, the first peer and second peer being communicated over a network;

performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer, wherein the first parameters being digital signature standard parameters;

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;

performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

2. (Original) The method according to claim 1 wherein the first certificate is a DSA type certificate.

3. (Original) The method according to claim 2 wherein the first and second parameters comprise a prime number $p_{dss}$, a prime number $q_{dss}$, a generator $g_{dss}$ and a public key for the first and second peers, respectively.

4. (Original) The method according to claim 3 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss} \wedge X_R \bmod p_{dss \text{ where }} X_R$ is a one-time private key from the second peer.

5. (Original) The method according to claim 4 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{SSK} = Y_{Adss} \wedge X_R \bmod p_{dss}$ where $Y_{Adss}$ is a DSS public key from certificate of peer A.

6. (Original) The method according to claim 5 wherein $Y_{Adss} = g_{dss} \wedge X_{Adss}$ mod $p_{dss}$ where $X_{Adss}$ is a DSS private key from certificate of peer A.

7. (Original) The method according to claim 5 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{SSK} = Y_R \wedge X_{Adss}$ mod $p_{dss}$ where $X_{Adss}$ is a DSS private key from certificate of peer A.

8. (Original) The method according to claim 1 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

9. (Currently Amended) An article of manufacture comprising:

a machine accessible medium including data that, when accessed by a machine, causes the machine to perform operations comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters;

performing a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer, wherein the first parameters being digital signature standard parameters;

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;

performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

10. (Original) The article of manufacture according to claim 9 wherein the first certificate is a DSA type certificate.

11. (Original) The article of manufacture according to claim 10 wherein the first and second parameters comprise a prime number $p_{dss}$, a prime number $q_{dss}$, a generator $g_{dss}$ and a public key for the first and second peers, respectively.

12. (Original) The article of manufacture according to claim 11 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss}$ ^ $X_R$ mod $p_{dss}$ where $X_R$ is a one-time private key from the second peer.

13. (Original) The article of manufacture according to claim 12 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{SSK} = Y_{Adss}$ ^ $X_R$ mod $p_{dss}$ where $Y_{Adss}$ is a DSS public key from certificate of peer A.

14. (Original) The article of manufacture according to claim 13 wherein $Y_{Adss} = g_{dss} \wedge X_{Adss} \bmod p_{dss}$ where $X_{Adss}$ is a DSS private key from certificate of peer A.

15. (Original) The article of manufacture according to claim 13 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$ where $X_{Adss}$ is a DSS private key from certificate of peer A.

16. (Original) The article of manufacture according to claim 9 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

17. (Currently Amended) A system comprising:

a processor; and

a memory coupled to the processor, the memory containing program code that, when executed by the processor, causes the processor to:

provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters, the first peer and second peer being communicated over a network;

perform a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; the second parameters being digital signature standard parameters;

provide a second certificate and the first public key from the second peer to the first peer; the second certificate comprising a plurality of second parameters;

perform a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

18. (Original) The system according to claim 17 wherein the first certificate is a DSA type certificate.

19. (Original) The system according to claim 18 wherein the first and second parameters comprise a prime number $p_{dss}$, a prime number $q_{dss}$, a generator $g_{dss}$ and a public key for the first and second peers, respectively.

20. (Original) The system according to claim 19 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss} \wedge X_R \bmod p_{dss}$ where $X_R$ is a one-time private key from the second peer.

21. (Original) The system according to claim 20 wherein the second exponentiation operation to generate the shared secret key for the second peer is $Y_{SSK} = Y_{Adss} \wedge X_R \bmod p_{dss}$ where $Y_{Adss}$ is a DSS public key from certificate of peer A.

22. (Original) The system according to claim 21 wherein $Y_{Adss} = g_{dss} \wedge X_{Adss}$ where $X_{Adss}$ is a DSS private key from certificate of peer A.

23. (Original) The system according to claim 21 wherein the third exponentiation operation to generate the shared secret key for the first peer is $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$ where $X_{Adss}$ is a DSS private key from certificate of peer A.

24. (Original) The system according to claim 17 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

25. (Currently Amended) A method comprising:

receiving by a second peer a first certificate of a first peer including a plurality first parameters, the first peer and second peer being communicated over a network;

performing a first exponentiation operation to generate a first public key using at least one parameter of the plurality of first parameters and a first private key; the second parameters being digital signature standard parameters;

receiving a second certificate and the first public key, the second certificate including a plurality of second parameters;

performing a second exponentiation operation to generate a first shared secret key using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate a second shared secret key using the first public key and a private key.

26. (Original) The method according to claim 25 wherein the first certificate is a DSA type certificate.

27. (Original) The method according to claim 26 wherein the first and second parameters each comprises a prime number $p_{dss}$, a prime number $q_{dss}$, a generator $g_{dss}$ and a public key.

28. (Original) The method according to claim 27 wherein the first exponentiation operation to generate the first public key is $Y_R = g_{dss} \wedge X_R \bmod p_{dss}$ where $X_R$ is a one-time private key.

29. (Original) The method according to claim 28 wherein the second exponentiation operation to generate the first shared secret key for the second peer is $Y_{SSK} = Y_{Adss} \wedge X_R \bmod p_{dss}$ where $Y_{Adss}$ is a DSS public key.

30. (Original) The method according to claim 29 wherein $Y_{Adss} = g_{dss} \wedge X_{Adss} \bmod p_{dss}$ where $X_{Adss}$ is a DSS private key.

31. (Original) The method according to claim 29 wherein the third exponentiation operation to generate a second shared secret key is $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$ where $X_{Adss}$ is a DSS private key.

32. (Original) The method according to claim 25 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

33. (New) The method according to claim 1 wherein the network be one of a wireless network and a Bluetooth network.

34. (New) The system according to claim 17 wherein the network be one of a wireless network and a Bluetooth network.

35. (New) The method according to claim 24 wherein the network be one of a wireless network and a Bluetooth network.